ABSTRACT

A method, apparatus and system may monitor system integrity in a trusted computing environment. More specifically, in one embodiment, an integrity monitor in a root virtual machine ("VM") may monitor guest software in a guest VM. The integrity monitor may securely maintain baseline information pertaining to the guest software and periodically (at predetermined intervals and/or based on predetermined events) compare the current state of the guest software against the baseline information. If the current state of the guest software is deemed to be compromised, the integrity monitor may be configured to take appropriate action, e.g., restrict the guest VM's access to resources. Additionally, according to one embodiment, the integrity monitor itself may be verified to determine whether it has been compromised.